IoT Security: A Smart Hospital Implementation Scenario

Asad Abbas, Muhammad Mubeen, Maaz Bin Ahmad, Muhammad Khalid Khan

Graduate School of Science and Engineering, PAF - Karachi Institute of Economics & Technology, Karachi, Pakistan

Summary
The term "IoT" (Internet of Things) can be defined as many small physical objects (having capability of sensing something from environment) connected to each other via some interconnecting networks to collect, share and convey information [1]. With the help of these small interconnected sensors or objects, we can automate a certain systems [2]. A smart hospital can be an example in which doctors can monitor the symptoms of a patient remotely as Wireless Body Area Network in IoT environment [3]. There can be other potential usage of IoT which includes schools, Traffic and Agriculture etc. One of the very important aspects of IoT is security which is still an open issue. Most of the proposed architectures do not define data confidentiality and integrity in detail. In conventional networks AES encryption technique can be used for similar purpose [4] however it can't be used for small devices with limited power and processing capabilities [5]. In this paper, we propose an efficient security implementation for IoT system in a typical WBAN environment having low power and limited processing devices.

Keyword:
Internet of Things, Security, Wireless Body Area Networks

1. Introduction

There is a huge tendency of society towards an "Always connected" model as rising of rapid advancement in wireless technologies. Now a day's wireless networks are all around us, these wireless equipment which are interconnected over a traditional network like internet that forms an IoT environment which can be used to analyze the remote location in a timely, ordinary, consistent and cost effective manner. But when the devices are connected over traditional network then there is a need of security mechanism because an attacker can access and manipulate our information. Although traditional network has its own security mechanisms but they are not suitable for an IoT system[5].

Wireless Body Area Networks (WBANs)[6] is one of low power WLAN system which is being used in IoT systems, it is a sensor network which provides efficient and reliable infrastructure for healthcare system that includes implanted, non-implanted and wearable sensor devices for human body. These sensor devices are used to capture various symptoms of a patient like heartbeat, body temperature, blood pressure, respiration and ECG etc. and send these Symptoms to a Body Network Controller (BNC). BNC is a core component in a WBAN which has the capabilities of taking data from sensors, process it and forwards to a centralized e-Health server. An e-Health server stores real time data of patients which can be accessed by a doctor to monitor the health of a patient remotely.

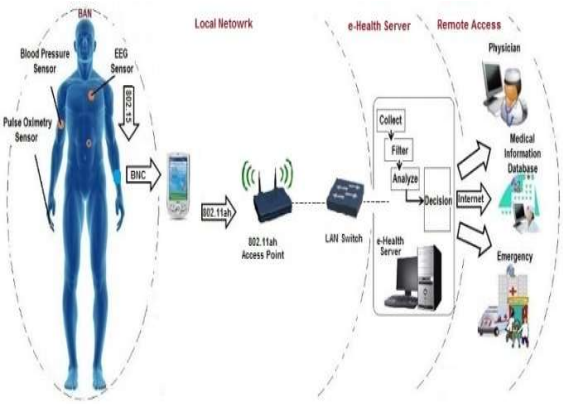

Figure 1 a BNC collects and processes data

As shown in figure 1 a BNC collects and processes data from the devices and forward it to a server using a wireless access network. The access network which is used in this scenario is WLAN IEEE 802.11ah. This standard is especially designed for IoT devices. There can be use of WLAN 802.11a/b/n standard but IEEE 802.11ah has some additional feature (like long range with low power). A comparison of various IEEE 802.11 standards is given in figure 2.

Multiple 802.11ah WLAN access points are installed at various locations in hospital vicinity. These access points are connected to an e-Health server via IEEE 802.3 Ethernet. As discussed earlier an e-Health server stores real time data of patients.

Manuscript received March 5, 2026
Manuscript revised March 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.3.15

TABLE 1: IEEE 802.11 COMMON WIFI STANDARDS BREAKDOWN

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

Figure 2 Multiple 802.11ah WLAN access points

This server is connected to a traditional network (internet). Which enable the doctors to access patient's data from remote locations. Like traditional network a security issue also arises here because BNCs are connected to e-Health server via wireless network in hospital which may have insider threats and same as an e-Health server which is connected to a public network which has outside attacker threat. So there is a need of security mechanism which secures the entire smart Hospital[3, 7].

Our major goals of this research are

(i) Access security of BNC and e-Health server
(ii) Data confidentiality
(iii) Authentication
(iv) Availability

As mentioned in abstract, traditional Networks make use of state of the art encryption algorithm 3DES, AES, IDEA etc. but these cannot be implemented in small devices with limited resources (in term of power consumption and processing capabilities) . We will try to implement AES with CTR (Counter) mode in BNC for encryption[7]. AES CTR keys are generated at server side and sent to BNC via a shared (private) key. This shared key is generated and configured in BNC at the time of patient registration. Encryption is performed by XOR operation of data with these CTR keys. These keys will be exchanged time to time when BNC is in ideal mode by using a shared key. XOR is logical operation and can be easily and efficiently implemented in small resource devices[8]. It is proven that AES CTR mode has same level of security as other modes. At other side e-Health server also makes use of public key algorithm for secure communication with remote users (Doctors). Each user has its own private key and will communicate with server by using a session key (session key is exchanged with the help of public key).
By using this scenario we can achieve access security of BNC and e-Health server, confidentiality, authenticity. Availability can be ensured by tracking the heartbeat of a patient, non-availability of heartbeat means there is an emergency or something is abnormal.

Section II of this research paper overviews the different existing communication protocol and their vulnerability in terms of security, Section III presents our proposed work and section IV concludes our research paper.

2. Related Work

Generally low power wireless devices fall in WPAN (Wireless Personal Arena Network) category. WPAN is specified in IEEE 802.15 standard in 2005. For wireless connectivity IEEE defines PHY and MAC layer specifications fixed, portable, and moving devices within a POS (personal operating space)[9]. POS is typically extends up to 10 m in all directions of an object, whether it is stationary or in motion. As shown in the figure 3 there are different technologies that are defined within WPAN:

(i) IEEE 802.15.1 is Bluetooth
(ii) IEEE 802.15.3 UWB
(iii) IEEE 802.15.4 ZigBee
(iv) IEEE 802.15.6 WBAN
(v) IEEE 802.11ah

Wireless technology	Standard	Network topology	Transmission range	Frequency	Bit rate	TX power	Security
ZigBee	802.15.4	star, cluster-tree, mesh	10 - 20 m	2.4 GHz	250 kb/s	−25 - 0 dBm	✓
Bluetooth	802.15.1	piconet, scatter net	10 - 30 m	13.56 MHz, 2.4 GHz	2.1 Mbit/s	0, 4, 20	✓
Bluetooth low energy	802.15.1	star	≈ 50 m	2.4 - 2.5 GHz	1 Mbit/s	0, 4, 20 dBm	✓
IEEE 802.15.6	802.15.6	star	< 100 m	NB, UWB, HBC	75.9 kb/s - 15.6 Mb/s	−25 - 0 dBm	✓
UWB	802.15.4a	piconet, peer-to-peer	10 m	3.1 - 10.6 GHz	480 Mb/s	−41.3 dBm/MHz	✓
WiFi	802.11	mesh	100 m	2.4 GHz	54 Mb/s	0 - 10 dBm	✓
Low-power WiFi	802.11ah	single-hop	100 - 1000 m	780, 868, 915, 950 MHz	150 kb/s	< 10 dBm or < 30 dBm, depending on the country	✓

Figure 3 WPAN (Wireless Personal Arena Network) category

Bluetooth is short range low cost technology, basically it was the replacement of wired peripheral devices such as keyboards, mouse, and headset. It is widely used for personal devices for data and voice[10]. Its typical range is 10 meter but it can be enhanced up to 100 meter with the help of amplifier[10]. The cipher algorithm used by Bluetooth is a stream cipher named E0. It required

resynchronization for every payload. The major components of E0 stream cipher are (i) payload key generator (ii) key stream generator and encryption and decryption part[11]. The size of encryption key can be vary from 8 bits to 128 bits depending upon mutual agreement between two communicating devices.Despite of these security mechanism, it is vulnerable or expose to Blue-snarfing, Man in the middle attack and Viruses[12].

UWB (Ultra Wideband) is an advance communication technology which supports high data rate with low power consumption but in short range[13]. UWB has the ability to penetrate through walls, doors and obstacles efficiently as well as carrying large amount of data in the form of pulses. These pulses are of short duration and are superimposed on carrier signal in a very time precisely manner across a very wide spectrum simultaneously. In perspective of WBAN, UWB is inefficient due two reasons. First UWB produces a high bandwidth radiation signal which is harmful to human body tissues. Second it is very difficult to manage high level of synchronization in WBAN compliance devices[14].

WBAN (Wireless Body Area Network) was basically designed for health monitoring system which is formed by small sensors to get the different symptoms of a patient[6].
It provides three level of security which are level 0 (unsecure communication), level 1 (authentication without encryption), level 2 (with both authentication and encryption)[15]. At the time of security adaptation a node and a hub needs to jointly select a security level. To encrypt the data a master key is generated by a one of the two communication parties. There are three type of keys MK (Master Key), PTK (Pairwise Temporal Key), and GTK (Group Temporal Key)[15]. It make use of public key algorithm named elliptic curve cryptography which is used for generating a MK. This public key algorithm keys are self-generated by parties involved in communication with no provision of digital certificate. Whole security mechanism is vulnerable to attack and also fails to provide forward security. Many attacks are feasible due to non-validation of public key. The attacks include impersonation attack and offline dictionary attack etc[15].

ZigBee is an extension of IEEE 802.15.4 WPAN standard developed by ZigBee alliance. The protocol stack of ZigBee is built on the top of IEEE 802.15.4[14] WPAN as shown in figure 4, which only define physical and MAC layer for low power personal area network [16]. The main characteristic are low power, low throughput, and long battery life with secure networking (128 bit AES encryption) [17].

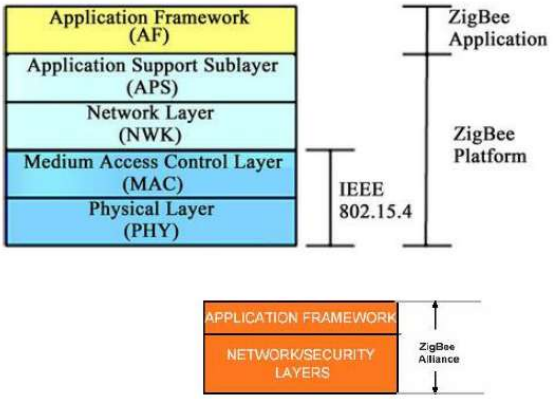

Figure 4 IEEE 802.15.4 WPAN standard

ZigBee network devices are coordinator, Router and End devices as shown in figure 5. Coordinator is a core component of a ZigBee network; it is always installed first to establish a ZigBee network. Router is a full function device as like coordinator but its prime responsibility is to extend network coverage but not to establish a network as coordinator. End device is not like coordinator or router because it cannot allow any device to join the PAN or assist in routing.

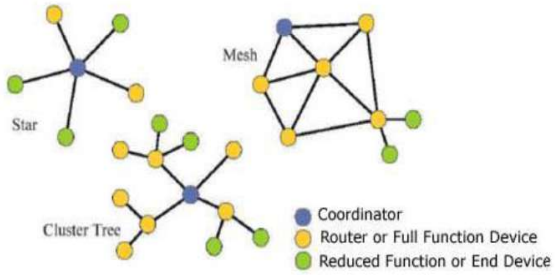

Figure 5 Router Full Function Devices

ZigBee make use of state of the art encryption algorithm AES (Advance Encryption Standard with 128 bit key). It provides security implementation on network layer and application layer[17].There are three kinds of keys to ensure security mechanism Master key, Link key and network key. Master key is preconfigured in the device before deployment. Its prime function is to secure

Manuscript received March 5, 2026
Manuscript revised March 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.3.1

the process of exchange the link keys between the two nodes. Link keys are to use to keep data confidentiality between nodes. In order to join ZigBee network each node must request current network key with the help of preconfigured master key (To avoid stealing of current network key). Network key is updated time to time by trust center and shared to all nodes by using old network key[18]. This whole security scenario works very well but it is insufficient in WBAN in term of resources (processing, power consumption). AES has a very complex encryption algorithm which requires high amount of processing to encrypt the data.

IEEE 802.11ah is the WLAN standard developed in 2014 and operates in 900 MHz in contrast with other wireless LAN standards[19]. The main idea behind this standard was to extend the range of IEEE802.11ac standard[20]. The use of low frequency band is not only beneficial in term of extending range but also low power consumption. Due to these features it is supposed best for IoT system. It can be used to connect many of sensors to server or conventional network. It enables the low power sensors to be operated without need of a power amplifier. It make use of low power MAC protocol which helps the sensor in lowering their power consumption. MAC protocol of 802.11ah has smaller frame format in contrast with other WLAN standards, priority assignment to sensor traffic and paging mode without bacon. It also has the ability to uniquely identify large numbers of station (sensors) in contrast other WLAN standards which is a prime requirement of an IoT system.

3. Proposed Work

To define our purposed idea it is important to get deep understanding of AES-CTR mode[21]. All modern block cipher operates in one of the five standard modes which are ECB, CBC, CFB, OFB and CTR. In CTR mode a variable called counter is initialized to IV (Initial Vector “some specified value”) which is incremented linearly or randomly (with the help of some pseudo random sequence). This value is wrap around to initial value upon reaching to its maximum allowable limit. The size of the counter depends upon variant of encryption algorithm being used, like for AES-128 the size of counter is 128 bit.

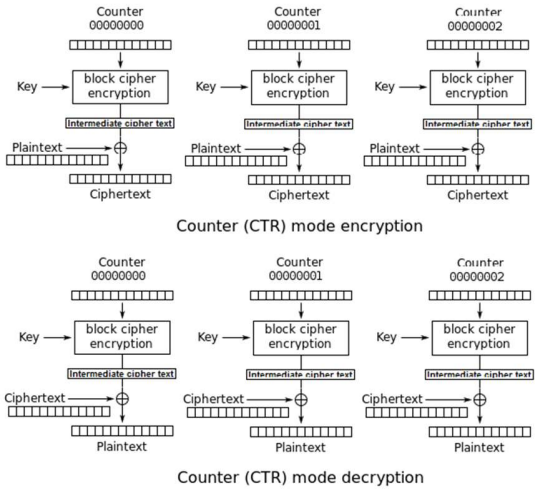

Figure 6

As shown in figure 6 sender will initialized the counter with IV. A key is also required to execute AES process and this key must be shared with receiver. First step is to encrypt the counter value with AES-128 encryption process by using shared key and production of Intermediate cipher text (term used for understanding in subsequent portion of the paper). If a gateway router encrypts its outgoing traffic with other modes such as CBC so much delay will be occurs which is not suitable for real time applications. Another benefit is, an intermediate cipher texts can be computed in advance and also in parallel. Because intermediate cipher text to be generated depends upon counter value that can be determine in advance. XOR operation is one of the fast logical operation which can be very efficiently implemented in hardware having very low latency in contrast with other arithmetic operation like multiplication[8]. CTR mode uses XOR operation for encryption at runtime but still obtaining the security of AES[21].

After getting deep understanding of AES-CTR[21] we are in the position to explain our idea. As shown in figure 7, when a patient is being admitted in hospital, its information is registered with e-Health server. Server will generate a unique patient ID (PID) and 128 bit intermediate cipher texts and will store against that patient. A BNC will also be configured against that patient and formerly generated intermediate cipher texts will be stored in BNC. BNC will be password protected to avoid any retrieval or modification of store

information by an adversary that can be a user of WBAN (patient), staff and visitor etc. All sensors which are deployed in WBAN of a patient are dedicated to a single BNC. It is noticeable that BNC has some permanent type of memory so it can store no of 128 bit intermediate cipher texts easily in our case these are 512. BNC will use these texts for encryption of data by XORing it with plain text data block as discussed earlier. Now BAN (BNC and sensors) is ready for deployment.

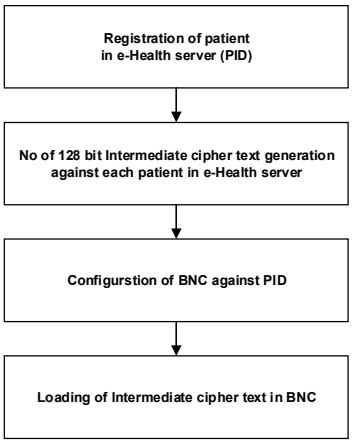

Figure 7 BAN (BNC and sensors) deployment.

Sensor will send these symptoms of a patient to its corresponding BNC. BNC will aggregate the data and sends to server. BNC is connected to IEEE 802.11ah access point which is further connected to e-Health server. As discussed earlier WBAN consist of various sensors and a BNC. These sensors capture different symptoms and send these to BNC. Although types of sensors can be vary from patient to patient but there are some symptoms which are mostly common to all patients like Heartbeat, Respiration and Blood pressure etc. Figure 8 shows various characteristics of a patient's symptoms.

As mentioned in abstract we have to provide confidentiality, integrity, authentication and access security to data between BNC and e-Health server. For encryption of data BNC will select an intermediate cipher text from its memory and will perform XOR operation with data as shown in figure 9.

Physiological Signal	Parameter range	Data arrival time (sec)	Sample Size (bits)	Data rate (kbs)
Blood flow	1-300 ml/s	0.025	12	0.48
ECG signal	0.5-4 mV	0.002	12	6.0
Respiratory rate	2-50breaths/min	0.05	12	0.24
Blood Pressure	10-400 mm Hg	0.01	12	1.2
Blood pH	6.8-7.8 pH units	0.25	12	.048
Nerve Potentials	0.01-3 mV	5E-05	12	240
Body Temperature	32-40 ^{0}C	5	12	.0024

Figure 8 Physiological Signals

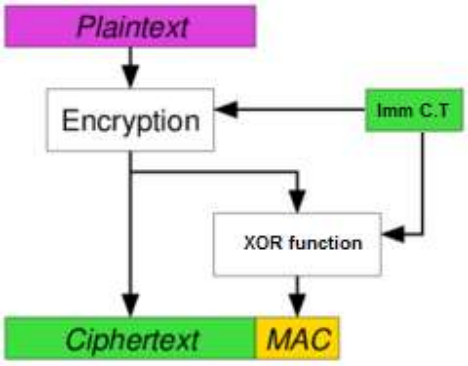

Figure 9 Encryption Algorithm

To provide confidentiality this whole 128 bit block is encrypted with one of selected Intermediate cipher text from memory and its reference is also attached with. Now data block is ready to be transmit towards server. It noticeable that if any adversary intercepts the data, it will be useless for him due to encryption as shown in figure 10

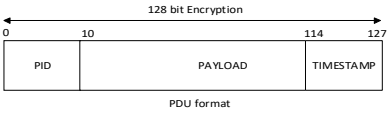

Figure 10 128-bits Encryption

For authentication process we have purposed a new authentication algorithm named CMAC (Compact MAC). CMAC is a simple, effective and easily implementable in low resources devices. As shown in the figure 11 our encrypted data consist of 128 bit. It will be divided into 4 octets and on each octet, left circular shit

Manuscript received March 5, 2026
Manuscript revised March 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.3.1

will be performed with predefined values. The amount of shift of each octet will be differs from other and will be predefined by server. These predefined values will be also configured in BNC. When bitwise XOR is performed on these octets mutually after left circular shift, a 32 bit value is obtained. This 32 bit is further XORed with least 32 bit of intermediate cipher text to obtain final 32 bit CMAC.

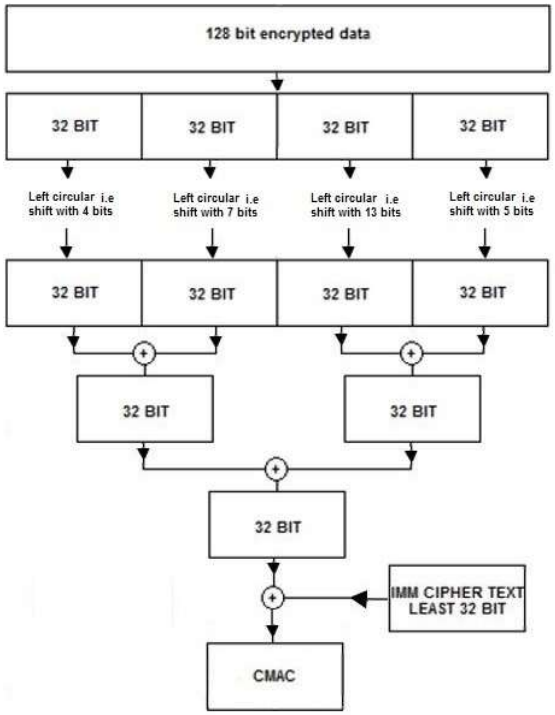

Figure 11 final 32 bit CMAC Algorithm .

This CMAC is attached with encrypted data. A complete PDU format is given below

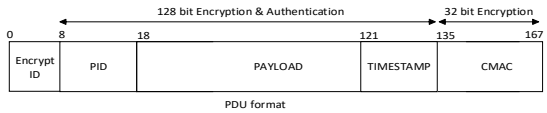

Figure 12 128-bits Authentication

At this point it is briefly defined how data will be encrypted and authentication will be provided. A field named encryption ID is attached with each PDU (Protocol Data Unit) as shown in figure 12 indicates particular intermediate cipher text which is used to encrypt this PDU. Receiver will use this field for selection of Intermediate cipher text to decrypt the PDU. After decryption of PDU receiver will check the PID at the start of payload and validate with stored PID against that particular BNC if validated then PDU has successfully decrypted otherwise rejected. For integrity and authentication check it will compute CMAC on received PDU and will compare it with received authentication data, if both found similar our PDU is authenticated and will be accepted. PDU also contains a timestamp field which enable the receiver to avoid from replay attack. Received PDU is also validated on timestamp, based on predefined time limit. It is noticeable that server will use same procedure stated earlier to send a packet to BNC. A BNC will adapt same procedure for decryption and authentication of the received packet. To ensure availability we will continuously monitor arrival rate of packet of certain BNC if we does not receive packets of certain BNC within predefined limit we will declare the emergency. The emergency indicates failure of one or more component of our network which may include LAN switches, Access Points and BNC etc. Another important aspect is determining the failures of the sensors, it can be achieved by monitoring symptoms in each arriving payload. If we don't receive any symptoms in our payload in predefined limit (as defined in figure 8). We can determine that a sensor is failed because when a sensor is failed it does not send data to BNC and BNC will send all zero's bits in its associated payload slot in the subsequent packets.

4. Conclusion

In this paper, we have reviewed different communication technologies for a smart hospital using IoT system and pointed out their vulnerabilities in term of security. We have purposed a simple efficient, secure and cost effective implementation for smart hospital. Our purposed work is more efficient and secure than any other implementations to the best of our knowledge. We have implemented state of the art AES encryption algorithm very efficiently which is feasible for resource-constrained devices. Our implementation not only fulfills the limitations of resource constrain devices which includes less processing capability, limited battery, limited memory and hardware simplicity but also provides a well-defined security mechanism which is prime requirement of today's networks. Our implementation ensures availability, authentication and data integrity with very simple but in effective manner.

References

[1] Atzori, L., A. Iera, and G. Morabito, *The internet of things: A survey.* Computer networks, 2010. **54**(15): p. 2787-2805.

[2] Zhu, Q., et al. *Iot gateway: Bridgingwireless sensor networks into internet of things*. in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*. 2010. IEEE.

[3] Fotouhi, H., A. Cauevic, and K. Lundqvist. *Communication and Security in Health Monitoring Systems--A Review*. in *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*. 2016. IEEE.

[4] . Hamalainen, P., et al. *Design and implementation of low-area and low-power AES encryption hardware core*. in *9th EUROMICRO Conference on Digital System Design (DSD'06)*. 2006. IEEE.

[5] . Boyle, D. and T. Newe. *Security protocols for use with wireless sensor networks: A survey of security architectures*. in *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on*. 2007. IEEE.

[6] . Jovanov, E., et al. *A WBAN system for ambulatory monitoring of physical activity and health status: applications and challenges*. in *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*. 2006. IEEE.

[7] . Saleem, S., S. Ullah, and H.S. Yoo, *On the Security Issues in Wireless Body Area Networks.* JDCTA, 2009. **3**(3): p. 178-184.

[8] . Tiri, K. and I. Verbauwhede. *A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation*. in *Proceedings of the conference on Design, automation and test in Europe-Volume 1*. 2004. IEEE Computer Society.

[9] . Sze-Toh, K.S. and K.C. Yow. *Usage of mobile agent in configuring WPANs*. in *Control, Automation, Robotics and Vision, 2002. ICARCV 2002. 7th International Conference on*. 2002. IEEE.

[10]. McDermott-Wells, P., *What is bluetooth?* IEEE potentials, 2004. **23**(5): p. 33-35.

[11]. Hager, C.T. and S.F. MidKiff. *An analysis of Bluetooth security vulnerabilities*. in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*. 2003. IEEE.

[12]. Panse, T. and V. Kapoor, *A review on security mechanism of Bluetooth communication.* International Journal of Computer Science and Information Technologies, 2012. **3**(2): p. 3419-3422.

[13]. Santhanam, M., *UWB technology and its application.* 2012.

[14]. Lee, J.-S., Y.-W. Su, and C.-C. Shen. *A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi*. in *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*. 2007. IEEE.

[15]. Toorani, M. *On vulnerabilities of the security association in the IEEE 802.15. 6 standard*. in *International Conference on Financial Cryptography and Data Security*. 2015. Springer.

[16]. Mulligan, G. *The 6LoWPAN architecture*. in *Proceedings of the 4th workshop on Embedded networked sensors*. 2007. ACM.

[17]. Baronti, P., et al., *Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards.* Computer communications, 2007. **30**(7): p. 1655-1695.

[18]. Vidgren, N., et al. *Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned*. in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. 2013. IEEE.

[19]. Aust, S., R.V. Prasad, and I.G. Niemegeers. *IEEE 802.11 ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi*. in *2012 IEEE International Conference on Communications (ICC)*. 2012. IEEE.

[20]. Sun, W., M. Choi, and S. Choi, *IEEE 802.11 ah: A long range 802.11 WLAN at sub 1 GHz.* Journal of ICT Standardization, 2013. **1**(1): p. 83-108.

[21]. Lipmaa, H., P. Rogaway, and D. Wagner. *CTR-mode encryption*. in *First NIST Workshop on Modes of Operation*. 2000.

Manuscript received March 5, 2026
Manuscript revised March 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.3.1